情報セキュリティ基本方針

株式会社金沢丸善（以下、当社）は、顧客情報、取引先情報、従業員情報を含む全ての情報資産を重要な経営資源と認識し、その適切な保護を事業活動の重要な課題の一つと位置づけています。当社は以下の方針に基づき、情報セキュリティを確保し、全従業員が一丸となってその取り組みを推進します。

1.経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。
全従業者に年 1 回以上の情報セキュリティ研修を実施します。

4.法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5.違反及び事故への対応

当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

制定日：2025 年 11 月 8 日

株式会社金沢丸善

代表取締役社長　野村　幸宏

対策基準

1. **情報資産の分類と管理**
    - 機密情報は暗号化し、特定の権限を持つ従業員のみがアクセス可能とする。
2. **アクセス制御**
    - 情報システムへのアクセスは、ユーザーID とパスワードによる認証を必須とする。
    - パスワードは、定期的（90 日ごと）に変更し、8 文字以上かつ英数字と記号を組み合わせる。
3. **ネットワークセキュリティ**
    - 社外から社内システムへ接続する場合は、VPN（仮想プライベートネットワーク）を利用する。
4. **データ保護とバックアップ**
    - 重要なデータは、毎日自動的にバックアップを取得し、別拠点の安全な場所に保管する。
    - バックアップデータの復旧手順を定期的に検証する。
5. **インシデント対応**
    - セキュリティインシデントが発生した場合、インシデント対応マニュアルに従い迅速に対応する。
    - 全てのインシデントは記録し、再発防止策を講じる。

情報セキュリティポリシー：実施手順

1. **情報資産の取り扱い手順**
    - 機密情報を取り扱う際は、必ず暗号化ソフトを利用する。
    - 紙媒体で機密情報を廃棄する場合は、委託先企業にて溶解を行う
2. **パスワード管理手順**
    - 新規アカウント発行時は、初期パスワードを必ず変更する。
    - パスワードは第三者に共有しない。疑わしいアクセスがあった場合は、速やかにパスワードを変更する。
3. **リモートワーク時のセキュリティ手順**
    - リモートワークを行う場合、業務に利用する端末には必ず最新のセキュリティパッチを適用する。
    - 公共 Wi-Fi の利用は禁止し、モバイルルーターまたは VPN を使用する。
4. **セキュリティインシデント報告手順**
    - インシデントを発見した場合、30 分以内に総務部へ報告する。
    - 報告内容には、インシデントの発生日時、影響範囲、初動対応内容を含める。